REMARKS/ARGUMENTS

I. Introduction

- Claims 1-16 remain in this application.
- Claims 1-16 stand rejected in this application.
- Claims 1 and 13-16 are rejected under 35 U.S.C. 102(e).
- Claims 2 - 12 stand rejected under 35 U.S.C. 112, second paragraph.
- Claims 2-12 are objected.

II. Amendments to the Specification

The sentence starting on page 18, line 12 was amended to correct a typographical error. The amendment corrects the word "book" to "codebook" when discussing the well known "electronic codebook (ECB) mode." Support for this change may be found in numerous books and articles published at the time of the current invention. (For an example from a reference provided by the Examiner, *see* Bruce Schneier, "Applied Crytography, protocols, Algorithms, and source code in c" 1996, John Wiley & Son, Inc. 2nd edition, pages 189-191).

The sentence starting on page 18, line 20 was amended to correct a typographical error. The amendment corrects the words "cipher blocking mode (CBC) mode" to "the cipher block chaining mode (CBC) mode." Support for this change may be found in numerous books and articles published at the time of the current invention. (For an example from a reference provided by the Examiner, *see* Bruce Schneier, "Applied Crytography, protocols, Algorithms, and source code in c" 1996, John Wiley & Son, Inc.

2nd edition, pages 193-197).

The sentence starting on page 18, line 5 was amended to correct a typographical error in which the letters "ed" were repeated at the end of the word "unencoded."

Because the specification was amended to correct the typographical errors, withdrawal of these objections are respectfully requested.

III. Amendments to the Claims

Claims 2-12 stand are objected to.

The examiner asked that acronyms in the claims be spelled out to avoid confusion with other claim characters. Applicant explicitly defined each and every acronym referenced in the claims in the specification of the present application. However, applicant has agreed to amend the claims to spell out each acronym the first time that it appears in the claims. Claim 2 was amended to spell out the "CBC"" acronym as "Cipher Block Chaining Prime." Claim 3 was amended to spell out the "CBC" acronym as "Cipher Block Chaining." Claim 4 was amended to spell out the "ECB" acronym as "Electronic Codebook."

Because the claims have been amended to avoid confusion with other claim characters by spelling out acronyms, withdrawal of these objections are respectfully requested.

IV. Rejections under 35 USC § 112

Claims 2 - 12 stand rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting an essential step. However, claims 2 – 12 are apparatus claims

containing no steps, therefore, no essential steps can be omitted.

A. Dependent Claim 2

In claim2, the examiner questioned what CBC' mode is. CBC' mode is a new cryptographic mode that prevents cut-and-splice attacks on 16 byte keys. Specifically, although the usual DES modes operate on 8 bytes of data at a time, CBC' allows DES to effectively operate on 16 byte units. Using CBC' mode, there is no risk that the first or second 8 byte blocks within the 16 bytes can be analyzed separately. This greatly increases the cryptographic strength of a security module. Specifically, CBC' mode is explicitly defined on page 19, lines 15 to 19 of the specification. Because CBC' is explicitly defined in the specification, withdrawal of this rejection for claims 2 – 12 is respectfully requested.

B. Dependent Claims 3-12

Applicant believes that claim 2 is now in condition for allowance for at least the reasons stated above. Claims 3-12 depend on claim 2 and hence contains all of the limitations of that base claim. Therefore, withdrawal of this rejection is respectfully requested.

V. Rejections under 35 U.S.C. § 102(e)

A. Independent Claim 1

Claim 1 stands rejected under 35 U.S.C. 102(e) as being anticipated by

Enichen et al. (U.S. Patent No. 6,333,983, hereinafter referred to as Enichen).

The focus in Enichen is to enable a cryptographic hardware module that is capable of 56 bit DES encryption to be used to support financial applications under the export controlled regime of the 1980's and 1990's, where encryption for the purpose of privacy was limited to 40 bits. Enichen teaches how to limit the capabilities of the strong cryptographic hardware to comply with export restrictions. Enichen discloses weakening the strong encryption provided by the cryptographic module by leveraging DES weak keys, to convert strong DES encryption to exportable 40 bit DES encryption by simulating a limited form of strong DES encryption using the MAC operations of the cryptographic module. Enichen's approach of weakening the hardware cryptographic module through changes to its software interface is in direct contrast to the approach of the present applications that changes to software should not weaken the hardware cryptographic operation. The present invention made sure that MAC operations would not be used to simulate strong encryption, key encrypting operations.

Applicant disagrees with the examiner that Enichen discloses "(f) key management functions; wherein said mode is determined by the hierarchical level of the key register . . . " Although Enichen suggests that different modes may be used to practice their invention, they clearly state that embodiments of the invention only use a single mode. (See Enichen, col. 13, lines 13 – 16 stating that "while the description has assumed a CBC mode of encryption and decryption, other modes such as the ECB mode could be used instead."). Because Enichen is practiced using only a single mode, Enichen does not disclose determining a

mode based upon the hierarchical level of a key register. Modes utilized in Enichen have no relationship to the hierarchical structure. Therefore, withdrawal of this rejection is respectfully requested.

B. Independent Claim 13

Claim 13 stands rejected under 35 U.S.C. 102(e) as being anticipated by Enichen. Specifically, the examiner claims that Enichen's discussion of cipherblock chaining mode (CBC) for encryption inherently teaches all of claim 13. (see Enichen, col. 3, line 61 to col. 4, line 11). Applicant believes that the Examiner has not sufficiently shown how the alleged inherent characteristics necessarily flow form the teaching of the applied prior art. Applicant would like the examiner to explain his technical reasoning on how "col. 3, line 61-11" supports the determination that the allegedly inherent characteristics necessarily flow from Enichen. "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." Ex parte Levy, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original) MPEP 2112.

Applicant would now like to explain why Enichen does not inherently anticipate or teach claim 13 regarding encryption. Claim 13 is not claiming CBC mode, but is instead claiming a CBC' mode (see disclosure, specification, page 19, lines 5 through 21). This mode is different than CBC mode. "CBC' is a new cryptographic mode which provides for secure encoding and decoding of

messages which are up to two blocks long, where the underlying encryption/decryption E/D (single-block) engine may be left unchanged." (Specification, page 19, lines 13 – 15). This mode solves a problem where CBC mode could fail at Level 2 when trying to chain blocks of "data" together. (See specification, page 19, lines 5 – 15). Basically, CBC' is immune to cut-and-splice attacks. In particular, it allows an encryption operation that generally operates on one word to be used as if it is a two-word operation, without risk that the individual words can be separately analyzed. This may be very important when using DES as the key encrypting operation to protect double-length DES keys (e.g., for triple-DES mode).

The following chart shows how CBC does not inherently anticipate or teach CBC' regarding encryption.

CBC	CBC'
$C1 = E(P1 \oplus IV)$	$C1 = E(P1 \oplus E(IV_i \oplus P2 \oplus E(P1)))$
$C2 = E(P2 \oplus C1)$	$C2 = E(P2 \oplus E(P1))$

Because CBC does not inherently teach or anticipate CBC' regarding encryption, withdrawal of this rejection is respectfully requested..

C. Dependent Claim 14

Claim 14 stands rejected under 35 U.S.C. 102(e) as being anticipated by Enichen. Applicant believes that claim 13 is now in condition for allowance for at least the reasons stated above. Claim 14 depends on claim 13 and hence

contain all of the limitations of that base claim. Therefore, withdrawal of this rejection is respectfully requested.

D. Independent Claim 15

Claim 15 stands rejected under 35 U.S.C. 102(e) as being anticipated by Enichen. Specifically, the examiner claims that Enichen's discussion of CBC decryption procedure inherently teaches all of claim 15. (see Enichen, col. 4, lines 11 - 19). Like stated in the discussion regarding claim 13, applicant believes that the Examiner has not sufficiently shown how the alleged inherent characteristics necessarily flow form the teaching of the applied prior art. Applicant would like the examiner to explain his technical reasoning on how col. 4, line - 19 supports the determination that the allegedly inherent characteristics necessarily flow from Enichen.

Applicant would now like to explain why Enichen does not inherently anticipate or teach claim 15. Claim 15 is not claiming CBC mode for decryption, but is instead claiming a CBC' mode for decryption (see disclosure, specification, page 19, lines 5 through 21).

The following chart shows how CBC does not inherently anticipate or teach CBC' regarding decryption.

CBC	CBC'
$P1 = D(C1) \oplus IV$	$P1 = D(C1) \oplus E(IV_i \oplus D(C2))$
$P2 = D(C2) \oplus C1$	$P2 = D(C2) \oplus E(P1)$

Because CBC does not inherently teach or anticipate CBC' regarding decryption, withdrawal of this rejection is respectfully requested..

C. Dependent Claim 16

Claim 16 stands rejected under 35 U.S.C. 102(e) as being anticipated by Enichen. Applicant believes that claim 15 is now in condition for allowance for at least the reasons stated above. Claim 16 depends on claim 15 and hence contain all of the limitations of that base claim. Therefore, withdrawal of this rejection is respectfully requested.

III. Conclusion

For all of the reasons advanced above, Applicant respectfully submits that the application is in condition for allowance and that action is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, the Examiner is requested to call Applicants' agent at the telephone number shown below.

The Commissioner is hereby authorized to charge any additional fees which may be required for this amendment, or credit any overpayment, to Deposit Account No. 501450.

In the event that an extension of time is required, or may be required in addition to that requested in a petition for an extension for time, the Commissioner is requested to grant an extension a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 501450.

Appl. No. 09/613,284
Amdt. dated July 1, 2004
Reply to Office Action of March 1, 2004

Respectfully submitted,

David G. Grossman
Registration No. 42,609

Date: July 1, 2004

Patent-Services.com
1408 Bayshire Lane
Herndon, VA 20170
(703) 338-6333